WYOMING DEPARTMENT OF AGRICULTURE
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS) POLICY

Effective Date: June 29, 2011

Policy Statement

(12.1.1) Payment card processing activities and related technologies must comply with the PCI-DSS in its entirety. All card processing activities must be conducted according to these requirements, no activity may be conducted nor technology employed that might obstruct compliance with any portion of the PCI-DSS. The standards and procedures are listed in the Related Documents portion of this Policy.

(12.1.3) This policy shall be reviewed annually by the Agency and State supporting agencies with the A&I division and updated as needed to reflect changes to business objectives or the risk environment.

Applicability and Availability

This policy applies to all employees. (12.1) Relevant sections of this policy apply to vendors, contractors, and business partners. The most current version of this policy is available at the Wyoming Department of Agriculture.

For programming not supported by the State of Wyoming A&I – ITD division the Agency will work with ITD and the Office of the Chief Information Officer (OCIO) to ensure proper wording is included in any vendor contracts for software purchase, installation or maintenance is in place to ensure compliance with PCI-DSS requirements and Agency Policies.

Related Documents

Payment Card Industry (PCI) Data Security Standard – Navigating PCI DSS version 1.2 dated October 2008 by the PCI Security Standards Council ™ attached to this policy.

PCI DSS\pci_dss.pdf

Job Required Cardholder Access Authorization Form attached to this policy.

Brand Recording Credit Card Security Policy attached to this policy.

PCI-DSS Requirement 1 & 2: Network Security
Install and maintain a firewall configuration to protect cardholder data

Firewall and router configuration standards (1.1) will be handled with Agency and A&I ITD support staff to ensure protection of card holder data. A current network diagram (1.1.2) will be maintained with this policy and updated with any changes in connections to cardholder data if data is ever entered into a computer (which is not occurring at this time). Testing of the external network connections and any changes to the firewall or router configurations (1.1.1) will be accomplished with recommendations from Agency IT staff and/or A&I – ITD in maintain PCI-

DSS compliance and done at least every six (6) months (1.1.6) if a computer is used for this purpose in the future.

A firewall will be established on every network connection in association with card processing activities (1.1.3), both between internal and external networks (1.2). Direct public access between the Internet and the system component in the cardholder data environment will be prohibited (1.3).

No wireless or mobile technology will be employed with cardholder processing without first ensuring that the firewall software and router configuration standards are met for PCI-DSS compliance. NO personal technology will be allowed with direct connectivity to the Internet or the agency's network.

Vendor-supplied defaults for system passwords and other security parameters

The agency will work with Agency ITD staff to ensure vendor-supplied defaults are changed prior to installing a system on the network; including but not limited to encryption keys, passwords and simple network management protocol (SNMP) community strings if a computer is used for this purpose in the future. Configuration standards for all system components will address all known security vulnerabilities and will be consistent with industry-accepted system hardening standards.

There will be one primary function per server. Unnecessary and insecure services and protocols will be disabled and unnecessary functionality removed such as scripts, drivers, subsystems, etc.

The State VPN system will be utilized for any web-based management and non-console administrative access if a computer is used for this purpose in the future.

PCI-DSS Requirement 3: Protect Cardholder Data

Protect stored cardholder data

Cardholder data will be shredded once the transaction has been completed via the secure phone line. Any transactions not process during a business day will be locked in a file cabinet and will be processed within 24 hours of receipt of such information, after which, the cardholder information will be shredded. At no time will records of card validation or value code and PIN data be stored after authorization.

PCI-DSS Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

The Agency will not transmit cardholder data through any computer or via any wireless networks.

PCI-DSS Requirement 5: Maintain a Vulnerability Management Program

Use and regularly update anti-virus software or programs

The Agency will use only anti-virus software suggested and employed by the State of Wyoming A&I – ITD division on all systems. All users with computers not directly tied to the State network will make sure they follow ITD recommendations in ensuring their anti-virus mechanisms are current and actively running. Any updates or changes to software suggestions will be implemented at the direction of A&I – ITD.

Develop and maintain secure systems and applications

Working with Agency IT staff and A&I – ITD the Agency will keep system components and software updated with the latest vendor-supplied security patches. Configuration standards will be updated as required by PCI-DSS Requirement 2.2. Any software development will be in accordance with PCI-DSS and based on industry best practices and incorporate information security throughout the software development life cycle. This will include:

- Testing of all security patches, and system and software configuration changes before deployment.
    - Validation of all input.
    - Validation of proper error handling.
    - Validation of secure cryptographic storage.
    - Validation of secure communications.
    - Validation of proper role-based access control (RBAC)
- Separate development/test and production environments.
- Separation of duties between development/test and production environments.
- Production data (live PANs) are not used for testing or development.
- Removal of test data and accounts before production system becomes active.
- Removal of custom application accounts, user Ids, and passwords before applications become active.
- Review of custom code prior to release to production in order to identify any potential coding vulnerability.

Change control procedures for all changes to system components will include documentation of impact, management sign-off by appropriate parties, testing of operational functionality and back-out procedures.

All web applications will be developed based on secure coding guidelines such as the *Open Web Application Security Project Guide* (OWASP). And will cover prevention of common coding vulnerabilities in software development with the current OWASP guide. Public-facing web applications will ensure protection against known attacks by review via manual or automated application vulnerability security assessment tools or methods at least annually or after any changes; or by installing a web-application firewall in front of public-facing web applications.

PCI-DSS Requirement 7, 8, and 9: Implement Strong Access Control Measures
Restrict access to cardholder data by business need to know

Access to system components and cardholder data will be limited to only those individuals whose job requires such access. Employees will have the least privileges necessary to perform their job responsibilities based on their classification and function.

Management and Agency head or designee, will sign an authorization form that specifies required privileges for all office personnel that will handle any credit card information. At this time access to charge cards is limited to the State Fair office staff and Fiscal section staff for entry of data and charging of cards.

The Agency will maintain copies of the signed authorization form. For systems not supported by the State of Wyoming A&I – ITD the form showing proper authorization will also be available when requesting vendors set up access to their programs for users that may contain cardholder data.

Assign a unique ID to each person with computer access

For every program that contains cardholder data information, whether maintained by the State or an outside vendor, a unique user ID and password will be required before accessing the level that contains card holder data. For remote access a VPN with individual certificates will also be required.

All passwords will be rendered unreadable during transmission and storage on all system components. Passwords will not show on user screens. Passwords will have to be changed at least every 90 days and will be at least 7 characters in length using both numeric and alphabetic characters. Users will not be able to submit a password that is the same as any of the last four passwords used. The system will lock the user out after not more than six attempts until an administrator enables the user ID. If a session is idle for more than 15 minutes it will require the user to re-enter the password to re-activate the terminal.

User access will be revoked immediately upon any termination of user needs and if the user account is not active for at least 90 days.

Restrict physical access to cardholder data

Appropriate facility entry controls will be used to limit and monitor physical access to systems in the cardholder data environment.

All unprocessed Credit Card Authorization forms containing PANs will be kept in a locked file cabinet. The portion of the form containing cardholder information will be shredded as soon as the information is successfully transmitted via the secure phone line.

PCI-DSS Requirement 10 & 11: Regularly Monitor and Test Networks

Track and monitor all access to network resources and cardholder data

The agency will work with Agency IT staff and A&I – ITD, or the OCIO for contract wording, to ensure a process for linking all access to system components to each individual user and have automated audit trails for individual accesses to cardholder data, actions taken by individuals with administrative rights, access to all audit trails, invalid logical access attempts, use of identification and authentication mechanisms, initialization of audit logs, and the creation and deletion of system-level objects. A record will be kept of at least the following audit trail entries for all system components: user identification, type of event, date and time, success or failure indication, origination of event, and the identity of name of the affected data, system component, or resource. Audit trails will be secure so they cannot be altered and retained for at least one (1) year, with a minimum of at least three (3) months immediately available for analysis.

Synchronization of all critical system clocks and times will be maintained. The Agency will work with Agency ITD staff and A&I – ITD to adhere to their recommendations in a process that will allow logs for all system components to be reviewed daily.

Regularly test security systems and processes

If the Agecny move to computer of credit card information, with assistance from A&I – ITD the Agency will assist in access to any wireless access points for at least quarterly testing, and to an Approved Scanning Vendor qualified by PCI Security Standards Council for quarterly external vulnerability scans. Quarterly internal vulnerability scans will be coordinated with A&I – ITD as well as scans conducted after network changes.

The Agency will work with A&I – ITD on the performance of external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. These penetration tests will include network-layer penetration test and application-layer penetration tests.

The Agency will work with A&I – ITD to ensure the use of intrusion detection system and/or intrusion prevention systems to monitor all traffic in the cardholder data environments and alert personnel of suspected compromises. All detection and prevention engines will be kept up-to-date.

With A&I – ITD the Agency will deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly.

PCI-DSS Requirement 12: Maintain an Information Security Policy
Maintain a policy that addresses information security for employees and contractors

The Agency is establishing this policy to publish, maintain and disseminate a security policy that addresses all PCI-DSS requirements and will be reviewed at least once a year and when updates in the environment change.

Each unit that accesses cardholder data on any point will develop operational security procedures that are consistent with requirements in this specification. Each unit will maintain an accurate inventory with proper device labeling that allows for quick identification of non-approved installations. Labeling will include device user, contact information and purpose.

Acceptable uses of technologies and network locations for technologies will be established with A&I – ITD along with a list of State-approved products.

Remote-access technologies will be set to automatically disconnect sessions after a specific period of inactivity.